REMARKS

The Examiner has rejected Claims 1, 3-5, 8, 10, 12-14, 17, 19, 21-23, 26, 28-29 and 32 under 35 U.S.C. 103(a) as being unpatentable over Bates et al. (U.S. Patent No. 6,785,732) in view of Liu et al. (U.S. Patent Publication No. 2002/0147780). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to each of the independent claims, the Examiner has relied on the Abstract; Col. 5, lines 51-57 and 65-67; Col. 6, lines 1-3 and 28-35; Col. 8, lines 1-3; Col. 9, lines 27-31; and Col. 11, lines 4-16 in Bates to make a prior art showing of applicant's claimed "retrieving code operable to pre-emptively retrieve via said internet link addressed data that would be accessed by a user following said at least one internet address" and "scanning code operable to scan said addressed data for malware" (see the same or similar, but not identical language in each of the independent claims). Specifically, the Examiner has argued that Bates teaches "checking e-mails and their attachments, downloaded files and websites or any contained links for possible viruses."

Applicant respectfully asserts that scanning e-mails, files and websites for viruses and merely mentioning links as sources for known viruses, in the context taught by Bates, does not meet applicant's specific addressed data. First, when read in context, applicant's addressed data is that which is "pre-emptively retrieve[d] via said internet link" and "would be accessed by a user following said at least one internet address" (see the same or similar, but not identical language in each of the independent claims). Clearly, the e-mails and files disclosed in Bates are not retrieved via an internet link, as claimed by applicant. In addition, Bates does not disclose that such e-mails or files would be accessed by a user following said at least one internet address, in the manner claimed by applicant.

Second, applicant respectfully asserts that, in Bates, checking web pages for viruses does not include scanning addressable data for malware, in the context claimed by

applicant. Specifically, Bates only teaches that "the uniform resource locator (URL) for the web page and for all links on the web page are compared to a list of known URL's in the virus information database 138 that were previously sources for viruses" (Col. 10, lines 58-63). Thus, Bates does not teach scanning addressable data, as applicant claims, but merely teaches comparing a URL with a database of URL's known to have previously contained viruses.

Third, Bates only teaches links that have been labeled as a source for known viruses. Clearly, identifying links as a source for known viruses does not meet "pre-emptively retriev[ing] via said internet link addressed data...to scan said addressed data," as specifically claimed by applicant (emphasis added). Thus, scanning e-mails, files and websites for viruses and merely mentioning links as sources for known viruses does not meet applicant's claimed "scanning code operable to scan said addressed data for malware" where such addressed data is "pre-emptively retrieve[d] via said internet link" (emphasis added).

Still with respect to each of the independent claims, the Examiner has relied on the following excerpt in Liu to make a prior art showing of applicant's claimed "storing logic operable to store result data identifying at least addressed data in which malware was not found" (see the same or similar, but not identical language in each of the independent claims).

> "[0037] When the recipient's email gateway 338 receives the scanned and cleaned email message from the group of email-scanning servers 340, the recipient's email gateway 338 determines that the email message is free of virus by checking the source of the email message or the status code in the header of the email message. The recipient's email gateway 338 includes a Post Office Protocol (POP) and/or Internet Message Access Protocol (IMAP) server so that virus-free email messages can be stored therein until the recipient at the device 342 requests the virus-free or clean email message. When such request is made, the recipient at the device 342 retrieves the virus-free email message from the recipient's email gateway 338. One skilled in the art would recognize that other mail server protocols may also be used."

Applicant respectfully asserts that Liu expressly discloses that the e-mails are "scanned and cleaned" prior to being stored (emphasis added). Thus, Liu does not meet applicant's claimed "addressed data in which malware was not found." Furthermore, merely storing "virus-free email messages," as in Liu, does not even suggest "stor[ing] result data **identifying** at least addressed data in which malware was not found," as claimed by applicant (emphasis added).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has included the following highlighted claim language in each of the independent claims:

> "(i) address identifying code operable to identify within currently held data at least one internet address associated with said currently held data;
>
> (ii) retrieving code operable to pre-emptively retrieve via said internet link addressed data that would be, but has not yet been, accessed by a user following said at least one internet address, after identifying within said currently held data said at least one internet address associated with said currently held data;

(iii) scanning code operable to pre-emptively scan said addressed data that was pre-emptively retrieved utilizing said internet link for malware; and

(iv) storing code operable to store result data identifying at least addressed data in which malware was not found;

wherein said addressed data is cached ~~when it~~after said addressed data has been pre-emptively retrieved and pre-emptively scanned, but before said addressed data has been accessed by said user" (see the same or similar, but not identical language in each of the independent claims).

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, especially in view of the amendments made hereinabove to each of the independent claims. A notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. Just by way of example, with respect to Claim 3 et al., the Examiner has relied on Col. 6, lines 4-20 in Bates to make a prior art showing of applicant's claimed technique "wherein said address identifying code is operable to search within said currently held data for string data having a format matching a pointer to an internet address." First, applicant notes that Bates discloses a virus information database that includes a specification of known viruses. However, with respect to the database, Bates does not disclose "search[ing]...for string data having a format matching a pointer to an internet address," as claimed by applicant.

In addition, applicant respectfully asserts that such excerpt does not teach currently held data in the context claimed by applicant. Specifically, Bates discloses "warn[ing] a web client...that has requested a web page that includes links to a bad URL." Thus, in Bates, the web page is only requested, and is not currently held, as claimed by applicant. Applicant also notes that Figure 4 in Bates clearly shows that the

data is only currently held if no virus checking is required, such that a "search within said currently held data for string data having a format matching a pointer to an internet address," as applicant claims, would not be performed in Bates (see operations 480 of Figure 4).

With respect to Claim 4 et al., the Examiner has relied on Col. 2, lines 11-35 and Col. 6, lines 21-25 in Bates to make a prior art showing of applicant's claimed technique "wherein said currently held data includes received e-mail messages." Applicant respectfully asserts that Bates does not teach e-mail messages in the context claimed by applicant. In particular, Bates only teaches detecting a virus within the e-mail itself or in an attachment to the e-mail. Furthermore, the only disclosure of a link in Bates relates to a requested web page (see specifically Col. 6, lines 15-20). Simply nowhere does Bates even suggest "identifying within said currently held data said at least one internet address associated with said currently held data" where "said currently held data includes received e-mail messages," as specifically claimed by applicant (emphasis added).

With respect to Claims 28 and 29, the Examiner has again relied on Col. 2, lines 11-35 and Col. 6, lines 21-25 in Bates to make a prior art showing of applicant's claimed techniques "wherein said currently held data is an e-mail and said internet address is an internet link embedded in said e-mail" (see Claim 28) and "wherein said currently held data is a file and said internet address is an internet link embedded in said file" (see Claim 29). For substantially the same reasons as argued above with respect to Claim 4 et al., applicant emphasizes that Bates only discloses a URL associated with a requested web page, and not "an internet link embedded in said e-mail" or "an internet link embedded in said file," as specifically claimed by applicant (emphasis added).

With respect to Claim 30, the Examiner has relied on Col. 9, lines 66-67 and Col. 10, lines 1-2 in Bates to make a prior art showing of applicant's claimed technique "wherein said malware found actions include removing said at least one internet address from said currently held data." Applicant respectfully asserts that such excerpts only disclose that "infected attachment or attachments [within the e-mail] are deleted."

Clearly, deleting attachments does not meet applicant's claimed "removing said at least one internet address," as claimed by applicant (emphasis added).

With respect to Claim 31, the Examiner has rejected such language in conjunction with the rejection of Claims 9, 18, 27 and 30 without making a specific prior art showing of applicant's claimed technique "wherein addressed data determined to contain malware via said scan is cleaned and said clean addressed data is stored locally for access via said internet address." In making such a rejection, applicant respectfully asserts that the Examiner has failed to consider the full weight of applicant's claim language since such claim language is not present in Claims 9, 18, 27 or 30. Furthermore, applicant respectfully asserts that the Page 2, paragraph 38 in Hypponen, as relied on by the Examiner, only discloses a firewall, and does not even suggest "addressed data determined to contain malware," let alone where such addressed data "is cleaned and said clean addressed data is stored locally for access via said internet address," as specifically claimed by applicant (emphasis added).

With respect to Claim 32, the Examiner has only generally rejected applicant's claimed technique "wherein access to said addressed data is allowed if said result data associated with said addressed data identifies said addressed data as not containing malware and if said addressed data has not changed since it was last scanned" under Liu without providing a specific paragraph within Liu where such claim language can be found. Applicant respectfully asserts that simply nowhere in Liu is there even a suggestion of result data, let alone where "addressed data is allowed if said result data associated with said addressed data identifies said addressed data as not containing malware and if said addressed data has not changed since it was last scanned," as claimed by applicant (emphasis added).

Again, since at least the third element of the *prima facie* case of obviousness has not been met, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 33-34 below, which are added for full consideration:

> "wherein storing said result data identifying at least addressed data in which malware was not found includes storing said result data in a database with an associated date of last scan and at least one of a file size and a checksum associated with said addressed data in which malware was not found" (see Claim 33); and
>
> "wherein addressed data in which malware was found is cleaned and said clean addressed data is stored locally for access via an updated internet address that replaces said internet address" (see Claim 34).

Yet again, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The

Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P475/01.160.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100